

BASIC CONCEPTS

- Smart Contract is an agreement
 - define the rules and penalties
 - automatically enforce those obligations
- Smart Contract is a program
 - the code runs at some point
 - automatically validates conditions and do the processing

EXAMPLE – DIGITAL NOTARY

- Idea
 create a digital notary that stores fingerprint of documents as
 proofs of their existence
- Solution

 use Ethereum platform to create a Dapp



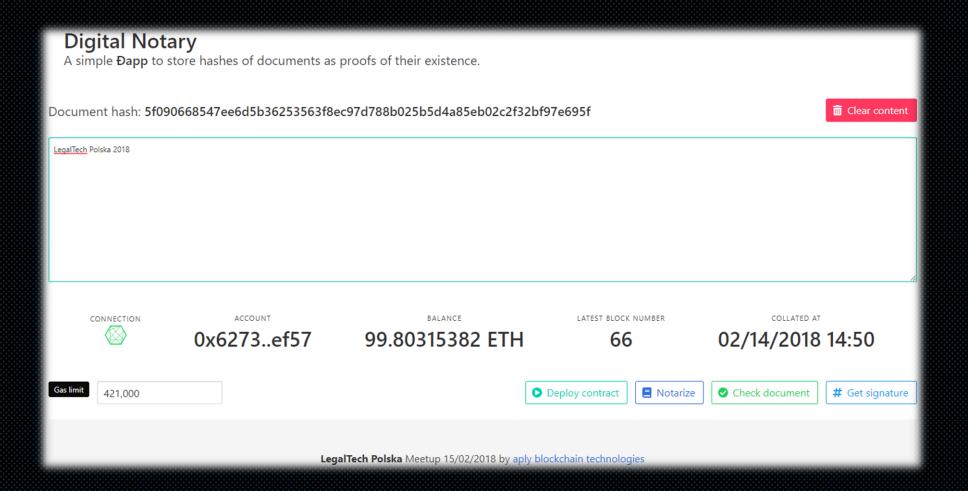
- Ethereum was designed as a smart contract platform
- EVM distributed global computer where all smart contracts are executed
- Using gas to limit the resources used by each contract
- Each operation costs gas paid in Ether
- Ethereum accounts pays for transaction but sets gas limit

THE CONTRACT

- Created with a programming language
 - Solidity, LLL, Serpent
- Has state and functions
- Interaction:
 - function calls or events

```
pragma solidity ^0.4.4;
// as proofs of their existence
contract ProofOfExistence {
 mapping (bytes32 => bool) private proofs;
 // Function to store a proof of existence in the contract state
 function storeProof(bytes32 proof) public {
   proofs[proof] = true;
 // Function to calculate and store the proof for a document
  function notarize(string document) public {
   var proof = proofFor(document);
   // store proof in a contract state
   storeProof(proof);
 // Utility function to get a document's hash (sha256 algorithm)
 function proofFor(string document) public pure returns (bytes32) {
   return sha256(document);
  // Function to check whether document was stored in a blockchain
 function hasProof(bytes32 proof) private constant returns(bool) {
   return proofs[proof];
  // Function to check if a document has been notarized
  // Returns boolean
 function checkDocument(string document) public constant returns (bool) {
   var proof = proofFor(document);
    return hasProof(proof);
```

POE - HANDS ON EXPERIENCE



IS IT AWESOME?

- Autonomy execution managed automatically
- Trust document are encrypted on a shared ledger
- Backup documents are duplicated many times over
- Safety encryption everywhere
- Speed software code that automates tasks
- Saving depending on use-case money may be saved
- Accuracy avoiding (human) errors

... IT'S NOT PERFECT

- It is still the code
 - ... and still has bugs
- It is not trivial
 - experienced staff needed to make the job done right
- Evolving technology
 - work in progress in many knowledge domains
- Stack
 - supplemented by technologies running the blockchain





DZIĘKUJEMY ZA UWAGĘ

tomasz.fidecki@aply.eu pawel.slawacki@aply.eu